UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF: **An LG Rebel 3 cellular phone, more particularly described in Attachment A, which is currently held at the FBI office located at 425 W. Nationwide Boulevard, Columbus, OH 43215**	**CASE NO:** 2:21-mj-414 **MAGISTRATE JUDGE:** Chelsey M. Vascura

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Gregory Meek (Your Affiant), a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

I. EDUCATION, TRAINING AND EXPERIENCE

1. I am a Special Agent (SA) with the Federal Bureau of Investigations (FBI) and have been since 2002. I am currently assigned to the Cincinnati Division, Athens Resident Agency.
2. During my career as a SA, I have been involved with the investigation of various cases and violations, ranging from criminal matters to counterintelligence and counterterrorism. I have also participated in the execution of numerous search warrants, including those involving searches and seizures of computers, digital media, software, and electronically stored information. As part of my duties as a Special Agent, I investigate criminal violations relating to child exploitation and child pornography violations, including the online enticement of minors, transportation of individuals for sexual activity, and the illegal production, distribution, transmission, receipt, and possession, of child pornography, in violation of 18 U.S.C. §§ 2251, 2252(a), 2252A, 2421 and 2422.
3. As a SA with the FBI, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other law enforcement agencies. I have not included in this affidavit all information known to me relating to the investigation. I have not withheld any evidence or information which would negate probable cause. I have set forth only the facts necessary to establish probable cause for a search warrant for the content of one LG Rebel 3 cellular phone which is currently held in the custody of the FBI Office, Columbus Resident Agency, located at 425 W. Nationwide Blvd., Columbus, OH 43215 (hereinafter referred to as the **SUBJECT DEVICE**).
5. The **SUBJECT DEVICE** to be searched is more particularly described in Attachment A, for the items specified in Attachment B, which constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. § 2421 – Transportation of an Individual for Unlawful Sexual Activity, 18 U.S.C. § 2422(b) - Attempted Coercion or Enticement of a Minor For Unlawful Sexual Activity, 18 U.S.C. § 2251 – Sexual Exploitation of Minors, 18 U.S.C. § 2252 – the Distribution, Receipt and Possession of Visual Depictions of Minors Engaged in Sexually Explicit Activity, and 18 U.S.C. § 2252A – the Distribution, Receipt, Pandering and Possession of Child Pornography. I am requesting authority to search the entirety of the **SUBJECT DEVICE**, wherein the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

II. APPLICABLE STATUTES AND DEFINITIONS

6. Title 18 U.S.C. § 2421 makes it a federal crime for any person to knowingly transport any individual in interstate or foreign commerce with the intent that such individual engage in any sexual activity for which any person can be charged with a crime.
7. Title 18 U.S.C. § 2422(b) makes it a federal crime for any person to knowingly use a means of interstate commerce to persuade, induce, entice, or coerce or attempt to persuade, induce, entice or coerce, any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person may be charged with a crime.
8. Pursuant to the Ohio Revised Code Section 2907.321, it is a felony under the laws of Ohio for any person, with knowledge of the character of the material or performance involved, to

create, direct, or produce an obscene performance that has a minor or impaired person as one of its participants.

9. Title 18 U.S.C. §2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.
10. Title 18 U.S.C. § 2252 makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.
11. Title 18 U.S.C. § 2252A makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

12. The term "child pornography"[1], as it is used in 18 U.S.C. § 2252A, is defined pursuant to 18 U.S.C. § Section 2256(8) as "any visual depiction, including any photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually conduct.
13. The term "sexually explicit conduct", as used in 18 U.S.C. §§ 2251 and 2252, is defined pursuant to 18 U.S.C. § 2256(2)(A) as "actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person." Pursuant to 18 U.S.C. § 2256(2)(B), "sexually explicit conduct" when used to define the term child pornography, also means "(i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (ii) graphic or lascivious simulated; (I) bestiality; (II) masturbation; or (III) sadistic or masochistic abuse; or (iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person."
14. The term "minor", as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as "any person under the age of eighteen years."
15. The term "visual depiction," as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to "include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image."
16. "Graphic" when used with respect to a depiction of sexually explicit conduct, means that viewer can observe any part of the genitals or pubic area of any depicted person or animal

1 The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

during any part of the time that the sexually explicit conduct is being depicted. (18 U.S.C. § 2256(10)).

17. The term "computer"[2] is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
18. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (such as writings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (such as printing or typing) or electrical, electronic or magnetic form (such as any and all digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).
19. "Internet Service Providers" (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
20. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.
21. As it is used throughout this affidavit and all attachments hereto, the term "storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

[2] The term "computer" is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones, digital watches, and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

IV. BACKGROUND REGARDING COMPUTERS, DIGITAL DEVICES, INTERNET

22. I know from my training and experience that computer hardware, computer software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.

23. Computers, mobile devices and the Internet have revolutionized the ways in which those with a sexual interest in children interact with each other and with children they seek to exploit. These new technologies have provided ever-changing methods for exchanging child pornography and communicating with minors. Digital technology and the Internet serve four functions in connection with child pornography and child exploitation: production, communication, distribution, and storage.

24. Computers, tablets and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including "GIF" (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

25. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

26. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 32GB. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Tablet devices have average storage capabilities ranging from 4 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 4 Gigabytes to 128 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

27. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service

Providers ("ISPs"). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers or cellular network; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol ("IP") addresses and other information both in computer data format and in written record format.

28. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography or seeking to exploit children online. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user's true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.

29. It is often possible to recover digital or electronic files, or remnants of such files, months or even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not

allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

30. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.
31. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.
32. A growing phenomenon related to smartphones, smart watches, and other mobile computing devices is the use of mobile applications. Mobile applications, also referred to as "apps," are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such "apps" include Snapchat, Skype, Meet24, Reddit, and Instagram.
33. Snapchat is a mobile application made by Snap Inc. ("Snap") and available through the iPhone App Store and Google Play Store. The Snapchat app provides users a way to share moments with photos, videos, and chats. Snaps are photos or videos taken using the Snapchat app's camera on an individual's mobile device, and may be shared directly with the user's friends, or in a Story (explained below) or Chat. Snap's servers are designed to automatically delete a Snap after it has been viewed by all intended recipients. Snap's

servers are designed to automatically delete an unopened Snap sent directly to a recipient after 30 days and an unopened Snap in Group Chat after 24 hours. A user can send messages, Snaps, audio notes, and video notes to friends within the Snapchat app using the Chat feature.

34. Skype is a communication service that transmits voice calls, video, and messages over the Internet, and was acquired by Microsoft Corporation, a company based in Redmond, Washington, in 2011. Skype can be installed and used on a desktop computer, laptop, tablet, or mobile phone, and is available through the iPhone App Store and Google Play Store. Skype users can make and receive local, long distance, and international phone calls; participate in video chats or send and receive video messages; send and receive short message system (SMS) text messages; and send and receive electronic files including documents, pictures, audio, and video.

35. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

36. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

    A. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This

sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

B. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

37. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices, as well as all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

VI. INVESTIGATION AND PROBABLE CAUSE

38. On April 4, 2020, the Athens County Sheriff's Office (ACSO) created a report indicating that Minor Victim, a 15-year-old female, was listed as a runaway juvenile. The report noted that Minor Victim had last been seen on or about April 3, 2020, in Millfield, Ohio. The ACSO asked that anyone with information regarding Minor Victim contact them immediately.

39. Approximately one year later, on or about April 27, 2021, the Athens County Prosecutor's Office (ACPO) received a Facebook message from Source 1 regarding the whereabouts and well-being of Minor Victim. The message included a link to a Facebook post created by an individual utilizing the Facebook username "Delilah Rose Price."

40. Law enforcement reviewed the post by "Delilah Rose Price" and noted that it began with the following statement: "I want to start this off with saying that I'm safe and have been

since I disappeared. I wanted to wait to pop up until I was a legal adult to insure [sic] that my biological family didn't have any say over me whatsoever."

41. The individual utilizing the "Delilah Rose Price" account then went on to include detailed claims of sexual abuse, indicating that "inhumane things" had happened to her. The Facebook post then stated that "the happiest day that I can remember there was the day that I knew I was getting out of that place." The post by the Delilah Rose Price user insisted that they had to leave for their own safety and that they were being "forced to be around incestuous pedophiles all day, every day."
42. Law enforcement also noted that the Facebook post specifically and explicitly referenced the family of the Minor Victim, referring to them by their surname, and stating that "they are a sick, sick family that likes to hide behind a religious cover and make everyone think they're the perfect bunch." Based on this and other content of the Facebook post, the ACPO had reason to believe that Minor Victim was the user of the Delilah Rose Price Facebook account and was responsible for the post about Minor Victim's whereabouts and prior family life. Thus, the ACPO issued a press release via Facebook asking for information about Minor Victim.
43. On or about April 27, 2021, an individual identifying themselves as Minor Victim contacted the ACPO, who then verified that she was in fact, the Minor Victim who had been missing. During that conversation, the Minor Victim provided detailed accounts of the sexual abuse she endured by her siblings while living in the home of her biological parents, all of whom she named.
44. Minor Victim told ACPO investigators that Minor Victim had reported the sexual abuse she had endured to her parents who failed to subsequently report that abuse to law enforcement or Athens's County Children's Services (ACCS). Minor Victim indicated that her biological parents continued to fail at protecting her and that she was continually sexually abused in her home. Because of this, Minor Victim stated that she reported the sexual abuse to ACCS in May of 2018 herself. Per the information provided by Minor Victim, ACCS ultimately closed the investigation and allowed Minor Victim to remain in the home with her abusers and parents.
45. Minor Victim further indicated that she suffered from psychological issues including self-harm coping mechanisms as a result of the ongoing sexual abuse. After a hospitalization in

September of 2018, ACCS removed Minor Victim from the home of her biological parents. Minor Victim informed ACPO that in October 2018, she was placed by ACCS into a foster residence. Minor Victim further indicated that despite being placed in a foster home, she continued to endure harassment by her biological family. As a result, she no longer felt safe in Athens County and had moved in and was currently residing with an individual by the name of JERRY Chadwick and his wife, SHAYNA Chadwick in Toombs County, Georgia.

46. In further communications with ACPO, Minor Victim reported that she first met JERRY in 2015 through an online gaming platform and utilized private chats on these forums to communicate with JERRY. In April 2020, Minor Victim and JERRY arranged for JERRY and SHAYNA to travel to Athens County, Ohio to pick Minor Victim up and bring her back to Georgia to reside with them.

47. ACPO then learned that just prior to Minor Victim moving in with JERRY and SHAYNA, a forensic extraction of Minor Victim's cell phone had been completed. More specifically, in January 2020, ACPO learned that the foster parents of then 15-year-old Minor Victim had taken Minor Victim's LG Rebel 3 cellular phone (**SUBJECT DEVICE)** to law enforcement based on their belief that Minor Victim had been taking and sending nude photographs of herself to adult males. The **SUBJECT DEVICE** was then voluntarily tendered to the ACSO and the foster parents of Minor Victim consented to a review of **SUBJECT DEVICE** for possible child pornography. On or about February 13, 2020, data from the **SUBJECT DEVICE** was extracted by ACPO. A subsequent review of that extraction revealed nude photographs of both males and females, but there were no identifying factors in those nude photographs and the individuals depicted in the photographs could not be recognized. At that time, the ACSO noted that the images could not be positively identified as child pornography. Because of that, on March 30, 2020, the ACSO closed the investigation citing an inability to determine that the images came from a direct source and lack of proof of a crime.

48. Following the April 2021 phone interview with Minor Victim and the knowledge that **SUBJECT DEVICE** possibly contained child pornography of Minor Victim, another review of the January 2020 forensic extraction was completed by the ACPO. In that review, ACPO noted the Snapchat application installed. Within the Snapchat application,

ACPO noted nude images depicting the Minor Victim that were sent from Minor Victim's account to a Snapchat user by the name of "JR Lee" later identified as JERRY's Snapchat account via JERRY's own admissions. Law enforcement further noted images that were sent to Minor Victim from JERRY. A preliminary review of those images, dated from September 2019 to November 2019, depicted nude photographs of JERRY and SHAYNA separately and JERRY and SHAYNA together, engaged in sex acts. Within that same preliminary review of Snapchat on the **SUBJECT DEVICE,** law enforcement also identified an account with username "Shayna Chadwick". In addition, law enforcement noted numerous sexually explicit Snapchat conversations sent by JERRY to Minor Victim.

49. Based on the information provided by Minor Victim and the forensic extraction previously completed by the ACPO of the **SUBJECT DEVICE**, law enforcement traveled to Toombs County, Georgia to speak with JERRY on May 5, 2021.

50. The ACPO met with JERRY at his residence and advised JERRY of his *Miranda* warnings. JERRY agreed to waive his rights and speak with law enforcement. During the conversation with the ACPO, JERRY admitted that he and Minor Victim had exchanged numerous nude photographs through the Snapchat and Skype mobile applications and that this exchange occurred when Minor Victim was still a minor living with her biological parents in Athens County, Ohio. JERRY indicated that the exchange of photographs began when the Minor Victim was around twelve years old. JERRY further admitted that the exchange of photographs with Minor Victim via Snapchat occurred again while Minor Victim lived with her foster parents in Ohio, just before Minor Victim came to live with him and SHAYNA in Georgia.

51. In that same conversation with ACPO, JERRY admitted that approximately two weeks after Minor Victim arrived in Georgia, when Minor Victim was seventeen years old, a sexual relationship began between himself and Minor Victim. JERRY indicated that the sexual relationship included oral and vaginal sex and that these sexual activities with Minor Victim have continued up until the day of the interview. JERRY then admitted his wife, SHAYNA, was also involved in sexual activities with Minor Victim. JERRY further indicated that SHAYNA also was involved and depicted in the exchange of nude photographs.

52. The ACPO then attempted to interview SHAYNA who requested her attorney and thus, the interview was immediately terminated.
53. Subsequent to interview on May 5, 2021, JERRY and SHAYNA were arrested by the Toombs County Sheriff's Office (TCSO) on charges of Marijuana Possession and Interference with Custody regarding Minor Victim. JERRY and SHAYNA remain in the custody of the TCSO pending local judicial process.
54. Your affiant then learned that the **SUBJECT DEVICE** was still located at the Athens County Sheriff's Office. **SUBJECT DEVICE,** more accurately described in Attachment A, was then obtained by your affiant with consent from ACPO on May 17, 2021. The device was subsequently transported to the FBI evidence room in the Columbus, Ohio Resident Agency, and has remained in law enforcement custody since the time it was acquired.
55. Based on the information that had been gathered to date by your affiant and ACPO, your affiant believes that there is probable cause that the **SUBJECT DEVICE** contains evidence of child exploitation activities perpetrated by JERRY and SHAYNA Chadwick.

VII. SEARCH METHODOLOGY TO BE EMPLOYED

56. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **SUBJECT DEVICE** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans, downloading or copying of the entire device, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant. Specifically, such techniques may include, but are not limited to:
    A. Examination of all of the data contained in any computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items listed in Attachment B;
    B. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items in Attachment B;
    C. Surveying various files, directories and the individual files they contain;
    D. Opening files in order to determine their contents;

E. Scanning storage areas;

F. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or

G. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

57. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

IX. CONCLUSION

58. Based on all the forgoing factual information, there is probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252, 2252A, 2421, and 2422 have been committed and that evidence, fruits and instrumentalities of these offenses will be found within the **SUBJECT DEVICE** listed in Attachment A, which is incorporated herein by reference. Your affiant therefore respectfully requests that the Court issue a search warrant authorizing the search of the **SUBJECT DEVICE** described in Attachment A, and the seizure of the items described in Attachment B.

Gregory Meek
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 15th day of June, 2021.

Chelsey M. Vascura
United States Magistrate Judge
United States District Court
Southern District of Ohio

ATTACHMENT A

PROPERTY TO BE TO BE SEARCHED

The devices to be searched are the following:

1. One LG Rebel 3, model number LGL158VL, black in color, MEID number 089758285603704724.

The item described above was obtained via consent from the Athens County Prosecutor's Office, Athens, Ohio and is currently being held at the FBI Office, Columbus Resident Agency, secure evidence storage location at 425 W. Nationwide Blvd., Columbus, OH 43215.

This warrant authorizes the forensic examination of the **SUBJECT DEVICE** for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

The following materials which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252, 2252A (possession, receipt, and distribution of child pornography), 2421 (transportation) and 2422 (coercion and enticement), including:

1. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or online storage or chat programs), utilities, compilers, interpreters, and communications programs.
2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, e-mail messages, chat logs, and electronic messages,) pertaining to the production, possession, receipt, or distribution of child pornography.
3. In any format and medium, all originals, computer files, copies, and negatives of child pornography and child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to digital files, e-mail messages, chat logs and electronic messages), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by cellular phone or computer, any child pornography.
5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications related to the sexual abuse or exploitation of minors.
6. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and

electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider or Electronic Communications Service.

7. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
8. Any and all visual depictions of minors, whether clothed or not, for comparison to any child pornography or child erotica found during the execution of this search warrant or obtained during the course of this investigation.
9. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.
10. Any Internet or cellular telephone communications (including email, social media, online chat programs, etc.) with others in which child exploitation materials and offenses are discussed, posted, and/or traded;
11. Any Internet or cellular telephone communications (including email, social media, etc.) with minors;
12. Evidence of the utilization of peer-to-peer file sharing programs;
13. Evidence of utilization of user names or aliases, email accounts, social media accounts, and online chat programs, and usernames, passwords, and records related to such accounts;
14. Evidence of software that would allow others to control the **SUBJECT DEVICE**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software and evidence of the lack of such malicious software;
15. Evidence indicating the computer user's state of mind as it relates to the crimes under investigation;
16. Evidence that any of the **SUBJECT DEVICE** were attached to any other digital device or digital storage medium;
17. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the **SUBJECT DEVICE;**
18. Passwords, encryption keys, and other access devices that may be necessary to access the **SUBJECT DEVICE**;

19. Records of or information about Internet Protocol addresses used by the **SUBJECT DEVICE;**

20. Records of or information about any Internet activity occurring on the **SUBJECT DEVICE**, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.